



FEDERAL PKI POLICY AUTHORITY

October 16, 2012 MEETING MINUTES

**USPS Headquarters
475 L'Enfant Plaza, SW
Conference Room: 4841
Washington, DC
9:30 a.m. – 12:00 a.m. EST**

9:30	Welcome, Opening Remarks & Introductions	Deb Gallagher, Chair
9:35	Discussion/Vote: September 2012 FPKIPA Minutes	Matt King
9:45	Discussion/Vote: IdenTrust Cross-Certification Application	Matt King
10:00	Discussion/Vote: FPKI CPS Approval Vote	Matt King
10:15	FPKI Management Authority (FPKIMA) Report	Darlene Gore
10:45	FPKI Certificate Policy Working Group (CPWG) Report	Charles Froehlich
	1. Discussion/Vote: PIV Content Signing Policy Change Proposal (Common CP)	
	2. Mapping Updates	
	3. Other Updates	
11:15	SHA-1 Transition Status	SHA-1 Affiliates
11:25	VA Status Update	John Hancock
11:30	FPKIPA Chair Update	Deb Gallagher
11:40	Other Agenda Items	Deb Gallagher
	<ul style="list-style-type: none"><i>If you cannot attend, please designate a proxy</i><i>Next FPKIPA meeting, November 6, 2012 – MEETING WILL BE AT GSA</i>	
12:00	Adjourn Meeting	Deb Gallagher

A. ATTENDANCE LIST

a. Voting Members

Organization	Name	T – Telephone P – In Person A – Absent
Department of Defense (DOD)	Mitchell, Debbie	T
Department of Energy (DOE)	Thomas, Michele	T
Department of Health & Human Services (HHS)	Slusher, Toby	T
Department of Homeland Security (DHS)	Miller, Tanyette (Proxy for Don Hagerling)	P
Department of Justice (DOJ)	Morrison, Scott	P
Department of State (State)	Rice, Barry	P
Department of Treasury (Treasury)	Wood, Dan (Proxy to DHS)	A
Drug Enforcement Administration (DEA CSOS)	Briggs, Sherrod (Proxy for Chris Jewell)	T
Government Printing Office (GPO)	Hannan, John	T
General Services Administration (GSA)	Gallagher, Deb	P
National Aeronautics & Space Administration (NASA)	Wyatt, Terry	T
Nuclear Regulatory Commission (NRC)	Sulser, David (Proxy to GSA)	A
Social Security Administration (SSA)	Mitchell, Eric	T
United States Postal Service (USPS)	Stepongzi, Mark	P
United States Patent & Trademark Office (USPTO)	Lindsey, Dan	A
Veterans Administration (VA)	Jurasas, Eric	A

b. Observers

Organization	Name	T – Telephone P – In Person A – Absent
Safer Institute	Boley, Ken	P
FPKIMA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
DoS (Contractor, ManTech)	Froehlich, Charles	P
FPKIPA (Contractor, Protiviti)	Jarboe, Jeff	P
FPKIPA (Contractor, Protiviti)	Silver, Dave	T
CertiPath	Spencer, Judy	P
ExoStar	Baker, George	T
DoD	Baldrige, Tim	T
FPKIMA (Contractor, Protiviti)	Louden, Chris	P
Entrust	Schoen, Isadore	T
Exostar	Cox, Jerry	P
CertiPath	Spencer, Judy	P

B. MEETING ACTIVITY

Welcome, Opening Remarks & Introductions, Deb Gallagher

The Federal Public Key Infrastructure Policy Authority (FPKIPA) met at USPS Headquarters, 475 L'Enfant Plaza, SW, Conference Room 4841, Washington, DC. Ms. Deb Gallagher, Chair, called the meeting to order at 9:35 a.m. EST. Those present, both in person and via teleconference, introduced themselves.

Discuss / Vote on September 11, 2012 FPKIPA Minutes, Matt King

There was a vote to approve the September 11, 2012 FPKIPA minutes. GSA motioned to approve; USPS seconded. The motion was approved unanimously.

Approval Vote for September 11, 2012 FPKIPA Minutes			
Voting members	Vote (GSA Motion; USPS Seconded)		
	Yes	No	Abstain or Absent
Department of Defense (DOD)	√		
Department of Energy (DOE)	√		
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ)	√		
Department of State (State)	√		
Department of the Treasury (Treasury) (Proxy to DHS)	√		
Drug Enforcement Administration (DEA CSOS)	√		
Government Printing Office (GPO)	√		
General Services Administration (GSA)	√		
National Aeronautics & Space Administration (NASA)	√		
Nuclear Regulatory Commission (NRC) (Proxy to GSA)	√		
Social Security Administration (SSA)	√		
United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO)			√
Veterans Administration (VA)			√

Discussion/Vote: IdenTrust Cross-certification Application - Matt King

IdenTrust submitted an application for cross-certification with the FBCA. Mr. Jerry Cox provided an overview of the IdenTrust PKI and a vote was held. USPS motioned to approve; DHS seconded. The motion was approved unanimously.



2012-10-01
fkipa_application_ID

Approval Vote for IdenTrust Cross-certification Application			
Voting members	Vote (USPS Motion; DHS Seconded)		
	Yes	No	Abstain or Absent
Department of Defense (DOD)	√		
Department of Energy (DOE)	√		
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ)	√		
Department of State (State)	√		
Department of the Treasury (Treasury) (Proxy to DHS)	√		
Drug Enforcement Administration (DEA CSOS)	√		
Government Printing Office (GPO)	√		
General Services Administration (GSA)	√		
National Aeronautics & Space Administration (NASA)	√		
Nuclear Regulatory Commission (NRC) (Proxy to GSA)	√		
Social Security Administration (SSA)	√		
United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO)			√
Veterans Administration (VA)			√

Discussion/Vote: FPKI CPS Approval - Matt King

Mr. Matt King explained that the FPKI certificate policies require FPKIPA approval of the FPKI Certification Practice Statement (CPS). The only changes made to the FPKI CPS since the last CPS version were in response to FPKI Trust Infrastructure auditor findings (discussed at the Fall 2011 FPKIPA meeting). Justice motioned to approve; Energy seconded. The motion was approved unanimously.



FPKI_CPS_v4_1_Red
acted_final_2012051!

Vote for FPKI CPS Approval			
Voting members	Vote (Justice Motion; Energy Seconded)		
	Yes	No	Abstain or Absent
Department of Defense (DOD)	√		
Department of Energy (DOE)	√		
Department of Health & Human Services (HHS)	√		
Department of Homeland Security (DHS)	√		
Department of Justice (DOJ)	√		
Department of State (State)	√		
Department of the Treasury (Treasury) (Proxy to DHS)	√		
Drug Enforcement Administration (DEA CSOS)	√		
Government Printing Office (GPO)	√		
General Services Administration (GSA)	√		
National Aeronautics & Space Administration (NASA)	√		
Nuclear Regulatory Commission (NRC) (Proxy to GSA)	√		
Social Security Administration (SSA)	√		
United States Postal Service (USPS)	√		
United States Patent & Trademark Office (USPTO)			√
Veterans Administration (VA)			√

FPKI Management Authority (FPKIMA) Report, Darlene Gore

Ms. Wendy Brown presented the FPKIMA report. The FPKIMA sent a survey to a number of agencies and had a relatively low (10%) response rate. The FPKIMA will look for ways to expand the survey – possibly by sending it through the CIO Council. The FPKIMA will continue to reach out and educate the FPKI Community about the FPKI and its services. Participation continues with US-CERT. The FPKIMA will be supporting the US-CERT help desk for PKI related matters. A meeting was held with DoD to discuss offline CA operations, and approaches will continue to be discussed at upcoming CPWG and FPKI TWG meetings. It was noted that a Verizon outage caused a spike in the FPKI repository response time in September. The next FPKI TWG meeting will be held on October 30, 2012.



Oct2012 Slides for
PA Meeting-final.pdf

ACTION ITEMS: None

FPKI Certificate Policy Working Group (CPWG) Report, Charles Froehlich

Mr. Charles Froehlich presented the CPWG Report.

a. Discussion/Vote: PIV Content Signing Policy Change Proposal

The CPWG discussed the *PIV Content Signing Change Proposal* and modifications proposed by DoD. Additional changes were added to sections 7.1.4 and 7.1.6 to include the *id-fpki-piv-contentSigning* policy OID. It was noted that as long as the Profile and Policy are updated, it is not a violation of FIPS 201 to include the PIV Content Signing OID. Changes to the Profile will include:

- Adding a new Profile for PIV Content Signing certificate that includes *contentSigning* EKU, and does not include any other EKU; and
- Removing the ability to include *piv-contentSigning* EKU on other certificates except where needed to align with FIPS 201 transition times (e.g., Common Devices will be allowed to have the *piv-contentSigning* EKU until it is no longer required by FIPS 201)

Costs will be included in system update costs to comply with FIPS 201-2. In addition, before these requirements become mandatory, *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program* will need to be updated, and changes to FIPS 201-2 must be accepted and published. Implementation of this change will require transition planning, but will occur

no later than 12 months after publication of FIPS 201-2. This change proposal will be finalized at the October 23, 2012 CPWG meeting.



Common Policy
Change Proposal PIV

b. Mapping Updates

The CP mapping for DoD was completed at the September 18, 2012 CPWG meeting and DoD is in the process of making the requested updates, changes, and clarifications. The final review is anticipated for the October 23, 2012 CPWG meeting. The CPWG has completed sections 1—7 of the ExoStar CP mapping and anticipates completing this mapping at its next meeting. The USPS CP mapping will begin at either the October 23, 2012 or November 1, 2012 CPWG meeting.

c. Other Updates

The CPWG will initiate discussion on a question raised by NIST (prompted from FIPS 201-2 comments NIST received) about the need to have the PIV/PIV-I Card printed name exactly match the certificate DN. CertiPath and DigiCert have raised questions on providing PIV-I for non-U.S. persons outside the U.S. issued by non-U.S. providers and not necessarily for access to U.S. Government facilities or systems. As a result of previous discussions, CertiPath and DigiCert agreed to provide a white paper on the subject outlining their requirements.

Due to the *PIV Content Signing Change Proposal discussion* and DoD and ExoStar CP mapping reviews, the FPKIPA-requested change proposal for more specific language into the FBCA and FCPCA CPs regarding use of digital signatures was postponed. Discussion of the change proposal is expected to begin at October 23, 2012 CPWG meeting.

SHA-1 Transition Status, SHA-1 Affiliates

CertiPath noted that SHA-1 transition planning is in progress and that Mr. Tim Polk will provide a briefing to CertiPath on SHA-1 to SHA-2 transitioning and NIST's opinion. Mr. Gary Wilson noted that SAFE is planning to migrate to SHA-2 in Q1 2013.

ACTION ITEMS: None

VA Status Update, John Hancock

Mr. King noted that he contacted VA and asked for an update. VA indicated they would call into today's FPKIPA meeting to provide a status. Since the meeting ended early and before VA called into the meeting, no update was received.

ACTION ITEMS: None

FPKIPA Chair Update, Deb Gallagher

Ms. Gallagher presented the FPKIPA Chair report. Upcoming meetings and events include:

Meeting	Date
Strong Logical Access Tiger Team (SLATT)	Wednesdays 10:00 – 11:00am
ISIMSC	October 17, 2012
CPWG	October 23, 2012
IAB	November 1, 2012
ICAMSC	October 24, 2012
FPKI TWG	October 30, 2012

Ms Gallagher gave an update on a variety of FICAM working groups. Highlights include:

- The FRAWG is reviewing the Trust Framework Provider Adoption Process, which includes how to get approved as a Trust Framework Provider.
- There are efforts to pool Mobility Working Groups across the government.
- The FCCX is partnering with USPS who will be the operating authority for the Federal Cloud Credential Exchange.



FPKIPA Chair
Report_16OCT12_DR

The next FPKIPA meeting is November 6, 2012. The meeting will not be at USPS, but rather at GSA and will start at 10:00 am EST to allow more time for members to vote.

Adjourn Meeting

Ms. Gallagher adjourned the meeting at 10:45 a.m. EST.

FPKIMA Open Action Items

Number	Action Statement	POC	Start Date	Target Date	Status
438	Ms Gallagher will publish the Digital Signature Guidance once a final review is complete; will be published on the web as well.	Deb Gallagher	12-Jul-11	13-Sep-11	Open
460	The FPKIMA will work with Mozilla to determine what Mozilla will accept if we do not provide CPSS	Wendy Brown	8-May-12	30-Jul-12	Open
464	Ms. Darlene Gore to provide the briefing that was given to the BOAC to Mr. Jeff Jarboe for distribution to the FPKIPA.	Darlene Gore, Jeff Jarboe	10-Jul-12	17-Jul-12	Open
466	Ms. Gallagher to forward complaints about some agencies not accepting external PIV-I and SHA-1 credentials to Ms. Deb Mitchell.	Deb Gallagher	10-Jul-12	17-Jul-12	Open
467	Mr. Slusher will draft language with Mr. Froehlich, Mr. King, and Mr. Silver, to add language about PKI uses and business processes to the FPKI Criticality letter and send the final version to Ms. Gallagher.	Toby Slusher	14-Aug-12	11-Sep-12	Open
468	Ms. Gallagher will submit the final FPKI Criticality Letter to the ICAMSC.	Deb Gallagher	14-Aug-12	30-Sep-12	Open
469	The FPKIMA will send information to the FPKIPA mail list about how to participate in the Mozilla discussion.	Wendy Brown	14-Aug-12	11-Sep-12	Open
470	Mr. Froehlich will lead CPWG discussions to develop a change proposal to add language to the FBCA and Common policies that requires digital signature of supporting documents	Charles Froehlich	14-Aug-12	11-Sep-12	Open
471	The CPWG will review the Common Policy to determine if another change proposal is required to allow for the long-term CRL issued by the Legacy Common Policy CA	Charles Froehlich	14-Aug-12	11-Sep-12	Open
472	Mr. Froehlich will lead discussions in the CPWG to develop a PIV Content Signing change proposal.	Charles Froehlich	14-Aug-12	11-Sep-12	Open

Number	Action Statement	POC	Start Date	Target Date	Status
473	Any Affiliate still cross-certified with the SHA1 FRCA needs to begin providing updates on their plans to transition off the SHA1 FRCA prior to December 31, 2013. This includes: DoD, DEA, Illinois, Symantec, CertiPath, and SAFE.	FPKI Affiliates	14-Aug-12	11-Sep-12	Open
474	Mr. Jason Miller will work to obtain more detailed information on the VA remediation efforts.	Jason Miller	14-Aug-12	11-Sep-12	Open
475	Ms. Gallagher will resubmit the metrics related to the FPKI Security Profile to the FISMA team	Deb Gallagher	14-Aug-12	11-Sep-12	Open